亚马逊云科技上的支付卡行业数据安全标准（PCI-DSS）V4.0

合规指南

2023/08 英文

2025/05 中文

亚马逊云科技

声明

客户需自行对本文件所含信息进行独立评估。本文件：

(a) 仅作信息参考用途；

(b) 描述当前亚马逊云科技（亚马逊云科技）产品服务与实践，可能随时变更，恕不另行通知；

(c) 不构成亚马逊云科技及其关联公司、供应商或授权方任何形式的承诺或保证。亚马逊云科技产品或服务按"现状"提供，不附带任何明示或暗示的担保、声明或条件。亚马逊云科技对客户的责任与义务受亚马逊云科技协议约束，本文件不构成且不修改任何亚马逊云科技与客户之间的协议。

(d)本指南是基于英文版本翻译的中文译本。如果中文译本的内容在解释或理解上与英文版产生任何差异、冲突或不一致，以英文版为准：https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws-v4-102023.pdf 。

PCI DSS 合规指引说明

本指南内容仅供信息参考。客户须自行完成 PCI DSS 合规认证。尽管客户可使用亚马逊云科技服务存储、传输或处理其持卡人数据（CHD），但亚马逊云科技不直接存储、传输或处理任何客户 CHD。本合规指南旨在协助客户在准备 PCI DSS 评估时，对其基于亚马逊云科技服务构建的持卡人数据环境（CDE）进行审查，不替代亦不更改亚马逊云科技 PCI 责任摘要（随 PCI DSS 合规证明 AOC 发布）的内容。

发布主体声明

本指南由亚马逊云科技全资子公司 Amazon Web Services Security Assurance Services, LLC（亚马逊云科技 SAS）提供。亚马逊云科技 SAS 是经 PCI SSC 认证的独立 QSAC（Qualified Security Assessor Company），依据 PCI DSS 保密条款及 PCI SSC 规则框架，向亚马逊云科技客户与合作伙伴提供 PCI DSS 合规实施指导，并可与 PCI 安全标准委员会（PCI SSC）或其他 QSAC 开展合规协作。

内容

摘要

本指南旨在协助客户规划并记录其亚马逊云科技工作负载在《支付卡行业数据安全标准》（PCI DSS）下的合规性，具体涵盖以下三方面内容：

- 控制措施选型：筛选符合 PCI DSS v4.0 要求的控制方案；
- 证据链规划：设计满足评估测试流程的证据收集机制；
- 合规沟通支持：向 PCI 资质安全评估机构（QSA）阐释控制措施实施细节。

本指南聚焦 PCI DSS v4.0 标准，当特定条款与 v3.2.1 版本一致时，将引用旧版内容。需特别说明的是，本指南不涉及 v4.0 与 v3.2.1 的版本差异分析，亦不区分 2025 年 3 月 31 日前视为最佳实践的要求与 v4.0 强制要求。此外，本指南仅针对 PCI DSS v4.0 中"明确定义的方法要求"（Defined Approach Requirements），不包含"自定义方法"（Customized Approach）选项相关内容。

如需从 v3.2.1 升级至 v4.0 的技术支持，可联系亚马逊云科技 SAS（亚马逊云科技安全合规服务子公司）或您的账户代表获取专项服务。

介绍

亚马逊云科技安全合规服务团队（亚马逊云科技 SAS）的核心使命是简化亚马逊云科技（亚马逊云科技）客户遵循《支付卡行业数据安全标准》（PCI DSS）的合规流程。我们与亚马逊云科技内部团队紧密协作，协助客户解决理解合规性要求、定位并实施解决方案、优化控制措施及评估流程等关键领域的挑战。基于客户高频咨询的 PCI DSS 合规基础问题，我们编制了《亚马逊云科技云上 PCI DSS v4.0 合规指南》。

本指南旨在为构建符合 PCI DSS 标准的应用程序提供概念框架与核心原则参考，所有章节均深度关联亚马逊云科技官方文档以支持技术落地并满足 PCI DSS 报告要求。需特别说明：本指南仅提供通用性合规建议，不针对任何具体客户的个性化场景提供解决方案。

本指南主要面向支付应用开发团队、云应用合规评估筹备团队，以及内部审计团队与 PCI 资质安全评估机构（QSA）专业人士。

PCI DSS 是一套旨在强化支付卡账户数据安全性的基线标准。账户数据包含持卡人数据（CHD）与敏感认证数据（SAD）：其中 CHD 涵盖主账号（PAN）、持卡人姓名、卡片有效期及服务代码；SAD 则包括完整磁道数据（或芯片等效数据）、CAV2/CVC2/CVV2/CID 验证码、PIN 码及 PIN 块。上述数据所在的整体环境称为持卡人数据环境（CDE），其系统组件涵盖与账户数据处理相关的人员、流程及技术。CDE 包含三类核心资源：存储、处理或传输账户数据的系统组件；与前者存在逻辑连接的系统组件；以及可能影响前两类组件及自身安全性的系统组件。这些系统组件的防护需通过周密规划实现 PCI DSS 控制措施的合规部署与验证。

PCI DSS 通过定义技术与运营基线要求保护账户数据。安全与合规是亚马逊云科技与客户的共同责任：客户需自主维护 CDE 范围并证明其合规性，而亚马逊云科技通过提供 PCI DSS 合规服务（如 EC2、S3 等）为客户赋能。亚马逊云科技 SAS 团队拥有行业认证评估师及 QSA 资源，可提供预评估活动指导、合规架构咨询及自动化合规最佳实践专业支持。如需获取亚马逊云科技云上工作负载的 PCI DSS 合规专项支持，请联系亚马逊云科技 SAS 团队。

PCI DSS v3.2.1 到 v4.0 变化

PCI SSC 从 PCI DSS v3.2.1 到 v4.0 存在诸多变更，这些更新可以分为三个类别：

需求变化	确保标准与新兴威胁和技术以及支付行业变化保持同步的变更。例如新增或修改的要求或测试程序，或移除某项要求。
澄清或指导	对文字、解释、定义、附加指导和/或说明的更新，以增强对特定主题的理解或提供进一步信息或指导。
结构或格式	内容的重组，包括合并、分离和重新编号要求以使内容保持一致。

关于 PCI DSS v4.0 的详细变更说明，请查阅 PCI 安全标准委员会（PCI SSC）发布的《PCI DSS v4.0 版本过渡时间表》及《PCI DSS 3.2.1 至 4.0 版本变更摘要》，更多技术文档可通过 PCI SSC 文件库获取。

亚马逊云科技服务 PCI DSS 合规性声明

作为 PCI DSS 认证的服务提供商（Service Provider），亚马逊云科技通过持续合规性验证助力客户满足其自身 PCI DSS 义务。在评估亚马逊云科技服务合规性时，我们默认客户数据可能包含信用卡号或敏感认证数据，且服务配置可能影响数据安全性。因此，通过 PCI DSS 认证的亚马逊云科技服务均被视为具备存储、处理或传输账户数据的能力，包括支撑服务运行的亚马逊云科技数据中心物理安全体系。

亚马逊云科技每年执行两次 PCI DSS Level 1 评估（服务提供商最高安全等级），评估完成后将向客户提供合规证明（AOC）。通过亚马逊云科技管理控制台的 Artifact 服务，客户可实时获取《亚马逊云科技 PCI 责任共担摘要》《亚马逊云科技合规证明》等文档，并查阅《合规计划覆盖的亚马逊云科技服务清单》。该清单动态更新已通过半年度 PCI DSS 评估的服务范围。

需特别提示：通过 PCI DSS 认证的亚马逊云科技服务虽可配置为合规解决方案，但客户需根据自身业务场景实施必要的额外控制措施。例如：客户可通过亚马逊云科技安全服务构建符合 PCI DSS 要求的持卡人数据环境（CDE），典型应用场景包括使用亚马逊云科技身份与访问管理服务（IAM）实施最小权限控制、通过 Amazon CloudWatch 与 亚马逊云科技 CloudTrail, 实现日志监控，使用 Amazon GuardDuty 检测恶意活动等。

更多亚马逊云科技安全服务技术实现方案，请访问亚马逊云科技安全博客获取更多内容。

亚马逊云科技责任共担模型

安全与合规是亚马逊云科技与客户的共同责任。亚马逊云科技责任共担模型（Shared Responsibility Model）通过全面管理基础设施层安全（涵盖主机操作系统、虚拟化层至数据中心物理安全），有效降低客户运营负担。

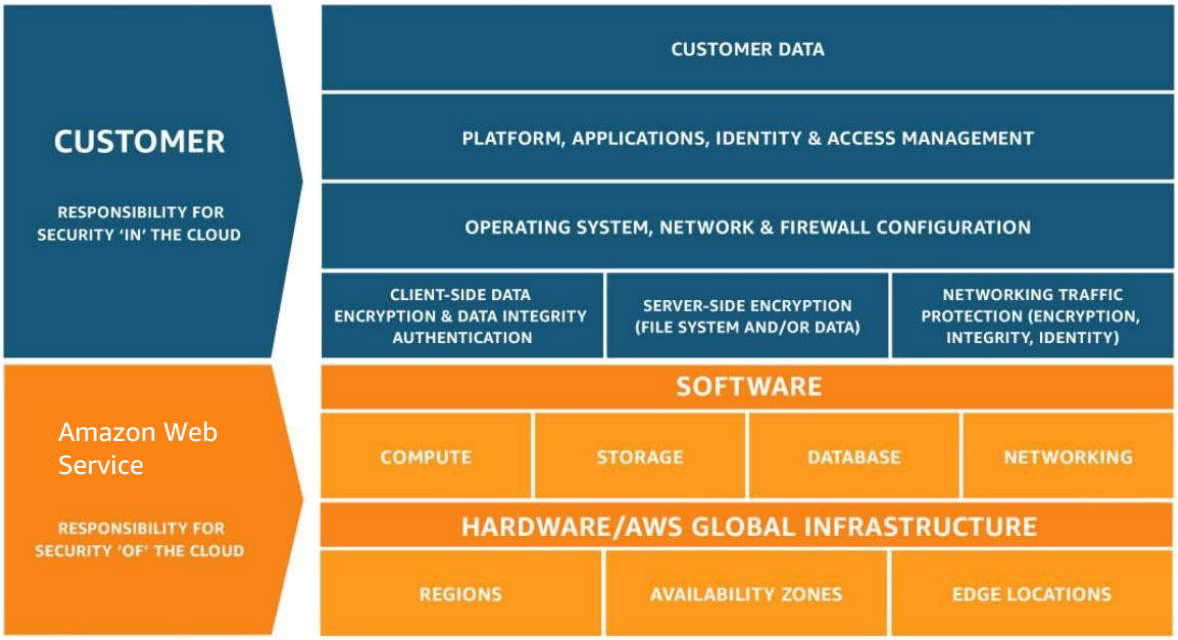

图 1 – 责任共担模型

如图 1 所示，亚马逊云科技负责"云本身"的安全合规，包括支撑云服务运行的全球基础设施体系。客户则承担"云中"配置系统的安全责任，具体范围取决于所选云服务类型，需根据 PCI DSS 要求对连接至持卡人数据环境（CDE）的系统组件实施合规配置。

亚马逊云科技云安全架构基于全球 24×7 监控的数据中心与定制化网络设计，满足涉密？机构的机密性、完整性及可用性要求。基础设施层包含硬件、软件、基础架构，通过物理隔离控制、多层级安全策略确保客户资源与数据的逻辑隔离。

对于部署在客户本地的亚马逊云科技 Outposts 混合云服务与亚马逊云科技 Snow Family 数据迁移设备，客户需自行承担硬件物理安全与环境控制责任。Outposts 作为全托管服务将亚马逊云

科技基础设施延伸至客户机房，亚马逊云科技 Snow Family 设备则支持离线大规模数据传输。两类服务均需客户直接管理硬件物理防护，不继承亚马逊云科技数据中心的环境控制体系。

客户拥有配置项决策权时，须按 PCI DSS 标准进行合规设置。亚马逊云科技将持续提供技术赋能，助力客户达成云上安全目标。

持卡人数据环境与范围

了解清楚账户数据在应用程序及环境中的完整流动路径（含与业务流程、程序代码的交互）是确定 PCI DSS 适用性、定义 CDE 边界及评估范围的核心前提。我们需要系统性分析数据流经的所有组件及其支撑系统，包括：

客户 PCI DSS 范围

PCI DSS 要求适用于三组资源：自身存储、处理或传输账户数据的系统组件，与前一组资源相连的系统组件，以及可能影响 CDE 安全的系统组件。

构成 CDE 核心的第一组资源是以某种形式存储、处理或传输账户数据的资源。这可能是传输包含账户数据的数据包的网络设备(物理或虚拟)，也可能是运行涉及支付或账户数据处理的业务逻辑的计算资源，或者是在任何时间段内保留账户数据的存储系统和服务。

在 PCI DSS 范围内，第二组系统组件被归类为"链接"组件。这些组件与构成 CDE(持卡人数据环境)核心的第一组资源之间建立了逻辑连接，这种连接可能是无限制的，也可能是配置数据流中明确定义的部分。例如，位于同一子网内且与存储、处理或传输账户数据的系统组件有无限制网络连接的服务器或容器都属于此类。此外，那些建立连接以收集非账户数据操作指标的监控系统等工具，也被包含在这一类别中。

PCI DSS 范围内的第三组系统组件是以某种方式影响 CDE 安全的组件。这些可能是直接或间接满足 PCI DSS 要求的工具或服务，如加密、入侵检测、审计日志记录和身份验证。它们还包括但不限于为 CDE 提供网络安全和边界分段的资源。

客户的 PCI DSS 范围可能超出其亚马逊云科技环境。客户可能拥有作为其 PCI DSS 环境的一部分，但未部署在亚马逊云科技上的系统，对于这些系统，客户仍然需要负责满足所有适用的 PCI DSS 要求。这可能包括零售场所、移动设备、办公室的管理系统或本地系统等系统和地理位置要求。

Scope 范围确定与验证

准确定义 PCI DSS 范围对于客户的安全态势和成功评估其环境至关重要。客户必须建立程序，通过识别账户数据的所有位置和数据流以及识别所有连接到 CDE 或可能影响 CDE 安全的系统，来确认其

PCI DSS 范围的准确性。他们必须确保这些系统包含在 PCI DSS 范围内，并至少每年(在年度评估之前)确认范围的准确性，并能够向其外部评估人员描述。

下图显示了 PCI DSS 范围内系统组件的考虑因素。

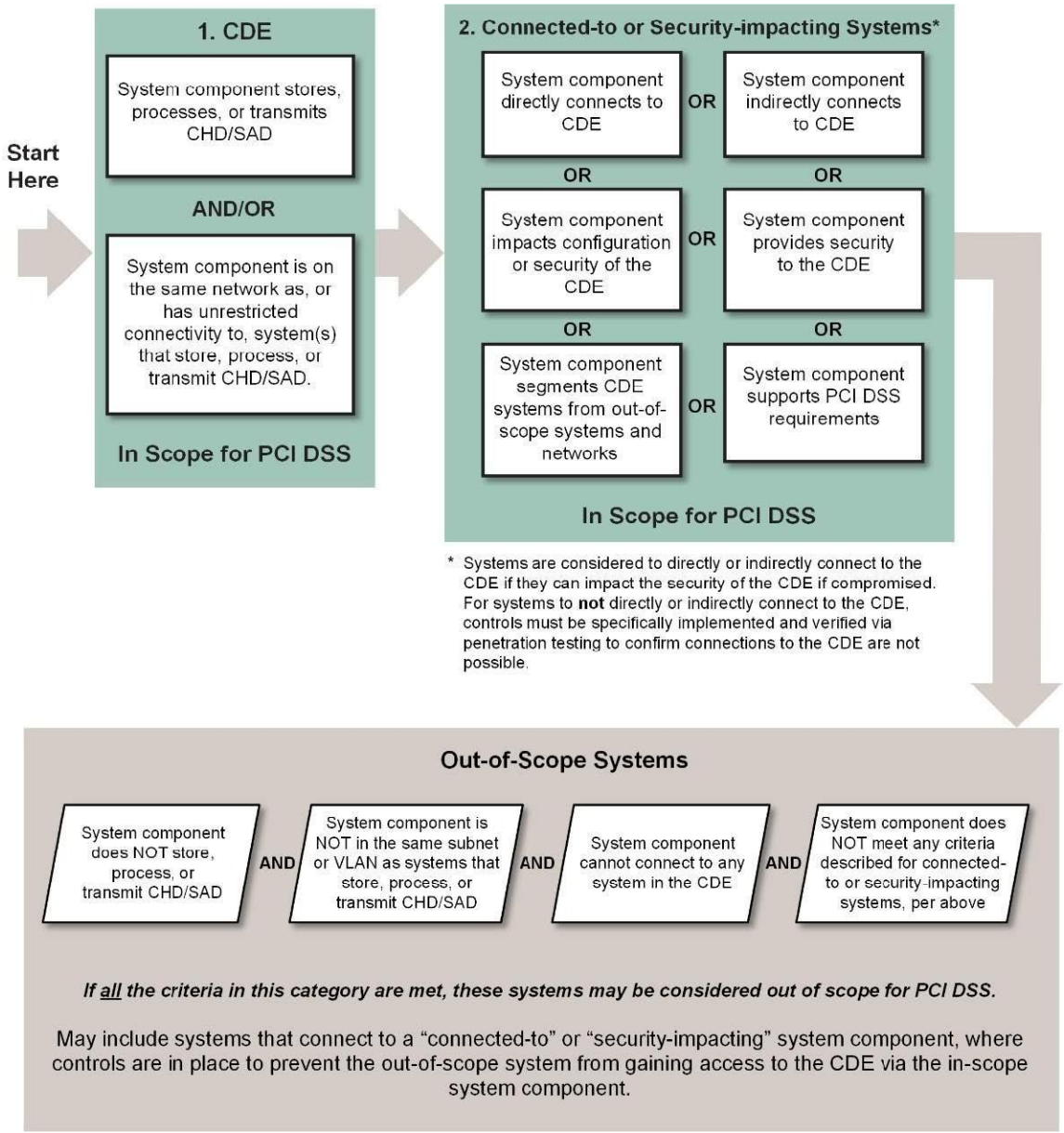

图 2 – 了解 PCI DSS 范围 （来源 PCI DSS 要求和测试程序 V4.0）(来源: PCI DSS: Requirements and testing procedures, v4.0)

涉及账户数据的业务流程和数据流的完整准确描述是规划和证明合规性的基础。账户数据应存储和处理在尽可能少的位置，以限制账户数据被滥用的风险，并限制客户评估范围。

分段隔离

分段隔离是保护持卡人数据(CHD)的重要安全控制方法，虽然不是明确的要求，但它可以显著限制客户的持卡人数据环境(CDE)和 PCI DSS 评估范围。分段可以通过多种物理或逻辑方法实现，例如正确配置的内部网络安全控制和访问列表，或其他限制对网络特定部分访问的技术。因此，列出现有机制非常重要，包括应用程序使用的和亚马逊云科技提供的机制。亚马逊云科技托管和抽象服务可能通过限制资源之间的连接，在限制客户 PCI DSS 范围方面发挥重要作用。每个 PCI DSS 合规的亚马逊云科技服务实例默认情况下都是隔离的，与其他资源分段，除非明确配置为其他方式。

许多评估人员可能不熟悉亚马逊云科技技术及其提供边界分段的能力。有关 PCI DSS 范围和分段的更多细节信息，请参阅《在亚马逊云科技上架构 PCI DSS 范围和分段》白皮书 （Architecting for PCI DSS Scoping and Segmentation on Amazon Web Services）。

使用电子商务外包服务的客户应遵循《信息补充：保护电子商务的最佳实践》（Information Supplement: Best Practices for Securing E-commerce.）。电子商务支付解决方案可能依赖于存储在商户环境中的组件，如 JavaScript(第 6.3 节案例研究三：部分外包)。这些资源，如 Amazon Simple Storage Service(Amazon S3 Amazon Simple Storage Service (Amazon S3))存储桶或 Web 服务器实例，都在评估范围内。如果客户正在完成 SAQ(自我评估问卷)，则可能需要 SAQ-A-EP。

图表和清单

需要识别和记录账户数据，以便对其进行适当保护。准确的网络拓扑图数据流图和完整的资产清单都是 PCI DSS 的强制性要求，也是确保您合规计划成功的关键因素。

数据流图

详细记录账户数据流非常重要，需要通过数据流图说明数据如何进入环境、存储位置以及如何穿越您的网络和系统组件。PCI DSS v4.0 的要求 1.2.4（对应 PCI DSS v3.2.1 中的要求 1.1.3）明确规定必须维护一份准确的数据流图。

这份数据流图在年度评估中，对于向评估人员证明范围确定过程的完整性和准确性也是必不可少的。您的图表和描述应具体指明资源名称，而不仅仅是服务名称。这些细节能够清晰地表明您环境中哪些资源需要遵守 PCI DSS 要求。

客户可以选择将数据流整合到一个全面的高级图表中，或者根据所涉及的应用程序和业务用例维护多个单独的详细图表。

以下是数据流图示例及相关的数据流索引：

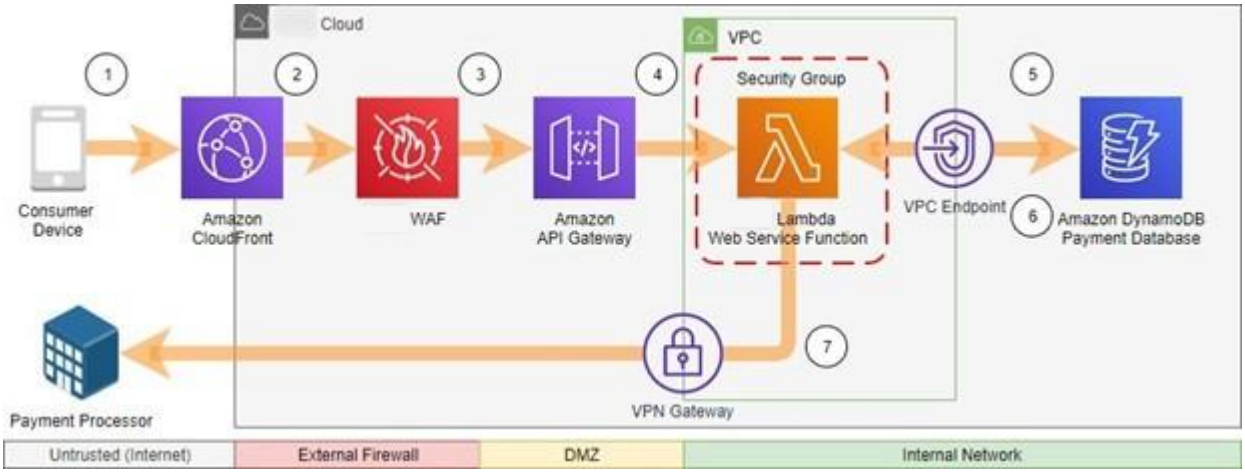

图 3 – 账户数据流程图示例

步骤	CHD 流程图目的	描述	传输	协议	访问控制	CHD/SAD	是否使用 TLS
1	授权	交易信息被发送至 Amazon CloudFront	Internet	TLS 1.2	发欺诈, 仅允许运行在 443 端口的 HTTPS 协议	PAN, 姓名, 过期时间, CVV2	否
2	授权	交易信息被被转发至 Amazon WAF	Amazon 网络	TLS 1.2	Amazon WAF 监听端口 (例如 443 端口), 基于状态的规则检查, 攻击规则	PAN, 姓名, 过期时间, CVV2	是
3	授权	交易信息被转发至 API Gateway	Amazon 网络	TLS 1.2	URL 参数规则 rules, 验证, 授权	PAN, 姓名, 过期时间, CVV2	Yes
4	授权	交易信息被转发至 亚马逊云科技 Lambda	Amazon 网络	私有网络	函数参数验证	PAN, 姓名, 过期时间, CVV2	NA

5	授权	交易信息被转发至 Amazon DynamoDB 支付数据库，用于储存交易之前的详细信息	私有 VPC	传输使用 TLS 1.2 协议存储使用亚马逊云科技 KMS (CMK)所支持的 AES-256 协议	安全组，位于 VPC 私有子网的 Amazon DynamoDB 端点，亚马逊云科技 API 证书，IAM 角色，资源策略	PAN，姓名，过期时间–保存支付方法	Yes
6	授权	交易返回给 Lambda 进行交易处理	私有 VPC	TLS 1.2	N/A – 相应流量	PAN，项目，过期时间–检索支付方式	N/A
7	授权	交易发送至支付处理商进行授权。不返回持卡人数据	互联网	IPSec VPN	由第三方服务提供商定义	PAN，姓名，过期时间，CVV2	由第三方服务提供商定义

图 4 – 账户数据流程示例

网络拓扑图

PCI DSS 在要求 1.2.3（对应 PCI DSS v3.2.1 中的要求 1.1.2）中规定必须维护准确的网络拓扑图。这些拓扑图对于理解持卡人数据环境(CDE)的范围和功能至关重要。它们应清晰展示以下信息：

- 网络和环境的边界
- 所有位置（零售点、数据中心、企业办公地点和云环境）
- 进出点 CDE 与可信和不可信网络之间通信点的网络访问和安全控制

可信网络是由组织或合规服务提供商控制和评估的网络。不可信网络包括所有其他网络，包括组织外部或未经组织评估的网络。这些图表还必须包括关键的范围内资源和技术，如亚马逊云科技 WAF 或 Amazon Elastic Cloud Compute Cloud (Amazon EC2)实例以及资源所在的不同子网。这还包括但

不限于分界点、相邻的范围外网络、保护 CDE 的安全组（security groups）和 AmazonVPC（Amazon Virtual Private Cloud）等项目。与数据流图类似，客户可以选择将所有项目整合到一个全面的高级网络拓扑图中，或维护包含所需元素的单独高级和详细网络拓扑图。这些图表还可以包括满足要求 1.2.4 所需的账户数据流。

系统组件和数据存储清单

亚马逊云科技服务可以根据云计算的三种主要模型（models for cloud computing:）分为以下三大类：

- 基础设施服务(IaaS)，如 EC2 实例。这些包含云 IT 的基本构建块，通常提供对网络功能、计算机(虚拟或专用硬件)和数据存储空间的访问。这还包括部署基础设施服务器的虚拟私有云(VPC)。
- 托管服务（PaaS），如 Amazon 关系数据库服务(Amazon Relational Database Service (Amazon RDS))和 Amazon 弹性容器服务(Amazon Elastic Container Service (Amazon ECS).)。亚马逊云科技负责托管服务的操作系统和底层环境。
- 抽象服务（SaaS），如 S3、Amazon DynamoDB 和 Amazon Lambda, 为客户提供由亚马逊云科技运行和管理的完整产品。亚马逊云科技管理底层环境以及代表您的持久性、恢复和可扩展性，并为您提供一个可使用的 Web 应用程序。

客户必须能够识别并列出其 CDE 中使用的系统组件类型。对于亚马逊云科技环境，这个列表包括实现应用程序功能、安全控制、环境管理的亚马逊云科技资源以及已连接的资源。这包括涉及存储、处理或传输账户数据的亚马逊云科技服务，也包括支持服务。

像 IAM 和 CloudTrail 这样的服务需要作为影响安全的服务包含在您的系统组件清单中。其他连接的服务可能包括 S3、Lambda 或 CloudWatch，用于处理和存储非安全日志，作为操作监控和报告机制的一部分。

我们建议您在系统组件清单中包含以下类似信息：

- 供应商(亚马逊云科技)
- 型号(亚马逊云科技服务名称)
- 系统组件或软件产品的名称以及版本或发布版本(如果服务有可选择的选项，例如 RDS MySQL)
- 提供的角色或功能(特定资源名称)

使用 Amazon Config, Amazon Systems Manager, Amazon Application Discovery Service.等服务可以收集更多信息。账户数据清单必须包括所有存储授权前和授权后账户数据的数据库、表格和文件(如适用)。第三方工具也可用于 Amazon Web Services 支付卡行业数据安全标准(PCI DSS) v4.0 on 亚马逊云科技进行清单收集。关于账户数据存储应捕获的详细信息包括以下内容：

- 数据存储名称(例如，亚马逊云科技服务、资源、数据库)
- 包含账户数据的特定文件或表格
- 存储的账户数据元素(例如，PAN、到期日、姓名、完整磁道数据、卡验证码/值和 PIN)
- 是否在授权前或作为发卡机构功能的一部分存储 SAD
- 安全详情(例如加密类型和强度、令牌化、访问控制和截断)
- 日志详情(例如日志管理解决方案的描述、应用程序级日志记录和接收日志数据的亚马逊云科技服务)

亚马逊云科技上 PCI DSS 合规指南

实现并维持 PCI DSS 合规可能是一项复杂且耗时的工作，而适当的规划有助于减轻这些负担。亚马逊云科技 提供了众多服务、工具、指导文档、白皮书和服务文档，以帮助减轻客户的负担。

亚马逊云科技 Well-Architected 架构框架

亚马逊云科技 开发了 亚马逊云科技 良好架构框架（Amazon Well-Architected Framework），帮助组织为其应用程序构建安全、高性能、弹性和高效的基础设施。安全支柱（Security Pillar）专注于保护信息和系统。关键主题包括数据的机密性和完整性、识别，以及管理谁可以通过权限管理做什么、保护系统并建立控制措施以检测安全事件。

最佳实践包括限制 亚马逊云科技 根账户的使用和访问、要求 亚马逊云科技 管理控制台账户使用多因素认证，以及实施最小权限原则。安全支柱对保护信息和系统的关注与许多 PCI DSS 技术要求条款相一致。您可以使用 亚马逊云科技 良好架构工具（Amazon Well-Architected Tool）来快速准备您的环境，使其符合 PCI DSS 标准。虽然该工具不能替代适当的预评估，但许多 亚马逊云科技 良好架构建议与许多 PCI DSS 要求条款的意图是一致的。

亚马逊云科技 良好架构透镜（Amazon Well-Architected Lenses）扩展了 亚马逊云科技 良好架构工具提供的指导，适用于特定行业和技术领域。客户可以审查适用于其持卡人数据环境(CDE)的相应透镜—如容器构建透镜（the Container Build Lens）、无服务器应用透镜（Serverless Applications Lens）或针对超出 亚马逊云科技 云范围的 CDE 的混合网络透镜（Hybrid Networking Lens）—以继续改善安全态势。

定制化方法

定制化方法是 PCI DSS v4.0 的新增内容，允许您以不严格遵循传统定义方法的方式满足 PCI DSS 要求条款。它使您能够专注于要求条款的目标而非严格的限制。它还允许您使用新技术和安全实践创新来展示您的安全控制如何满足 PCI DSS 要求条款。本指南不涉及任何要求条款的定制化方法可能性，因为它们每个客户环境都有其特定性，需要针对本白皮书所能解决的问题做更深入的风险审查和讨论。PCI DSS 附录 D （Appendix D to the PCI DSS）提供了使用定制化方法所需的详细信息。PCI DSS 还在附录 E 中包含两个示例模板：控制矩阵和目标风险评估。这些为理解所需的信息和文档提供了良好的起点。

目标风险分析

PCI DSS v4.0 引入了另一个新概念，称为目标风险分析，作为要求条款 12.3.1 和 12.3.2 的一部分。与传统的企业范围风险评估不同，目标风险分析有更精细且更集中的范围，独立于特定的 PCI DSS 要求条款。目标风险分析旨在识别适用于特定要求条款的资源、这些资源所面临的威胁以及潜在恶意事件发生的可能性。该分析还详细记录了推荐的解决方案、风险评估结果，并明确规定了执行各项要求条款的必要频率。

进行目标风险分析主要有两个原因。首先，它可以支持那些允许根据环境风险灵活调整任务执行时间的要求，比如数据安全标准中规定为定期执行的任务。为满足要求 12.3.1，必须进行这种目标风险分析来确定适当的执行频率。其次，当采用非预定义方式来满足 PCI DSS 要求时，目标风险分析可以支持使用自定义方法的合理性。

根据条款 12.3.2，必须对使用定制化方法的每个要求执行这些风险分析。所有目标风险分析必须至少每 12 个月审查一次，以确定目标风险分析的执行情况以及结果是否仍然有效。定义定期时间的风险评估年度审查应包括审查执行情况以及频率是否应该改变。

当用于支持 PCI DSS 要求条款的定制化方法时，风险评估需要与控制矩阵（或多个矩阵）、测试证据以及其有效性证据一起提供给您的评估人员。用于支持定制化方法的目标风险分析还必须包括高级管理层的书面批准和附录 D 中的证据要求。

重要的是要理解，亚马逊云科技 计算资源的潜在短暂性质以及大多数 亚马逊云科技 服务提供的抽象级别是您可以包含在风险评估中的缓解因素。同样，诸如 Bottlerocket（Bottlerocket operating system）等 亚马逊云科技 资源在针对 PCI DSS 恶意软件要求条款进行审查时，也提供了改进的安全性和资源利用率。

PCI DSS 要求条款

通过在设计应用程序时谨慎选择影响安全的服务和所需控制措施，您可以减少创建和维护持卡人数据环境(CDE)所需的工作量。以下我们将探讨不同的 PCI DSS 要求条款以及如何利用 亚马逊云科技 服务支持您的合规工作。

要求条款 1

第一个 PCI DSS 要求条款专注于网络安全和限制对 CDE 的网络访问。与传统的本地环境相比，客户可以利用 亚马逊云科技 软件定义网络服务，以新颖且高效的方式满足其网络和网络安全控制要求。

亚马逊云科技 网络边界

虚拟私有云(VPC)使您能够完全控制虚拟网络环境，包括资源放置位置、网络连接和安全。VPC 允许客户在 亚马逊云科技 云中配置逻辑隔离的部分，可在其中定义的虚拟网络中启动 亚马逊云科技 资源。亚马逊云科技 实施了 Edge 架构，分布并独立扩展了许多通常集成在传统防火墙中的功能。亚马逊云科技 还提供了多种服务，可帮助支持 PCI DSS 的网络和网络安全控制(NSC)要求。支持 PCI DSS 要求条款 1 的四个核心服务是 VPC、安全组、VPC 网络访问控制列表(VPC network access control lists 网络 ACL)和 IAM。

1.2 网络安全控制配置

根据此要求条款，客户负责配置和管理其安全组和网络 ACL，以及 VPC 网络组件，如路由表和互联网网关。

亚马逊云科技 Firewall Manager（Amazon Firewall Manager） 是一种安全管理服务，可帮助您集中配置和管理跨账户和应用程序的 NSC 规则。Firewall Manager 还可以通过创建策略来设置护栏，定义跨 VPC 允许和禁止的安全组，帮助您证明符合要求条款 1.2.7.b 和 1.2.8。

1.3 限制对 CDE 网络的访问

安全组是客户 VPC 内的有状态 NSC，通过控制每个虚拟弹性网络接口(ENI)的入站和出站流量，支持满足要求条款 1.3 和 1.4。安全组可用于按 IP 地址、端口和协议限制流量，并满足 PCI DSS 要求条款 1.2、1.3 和 1.4 的要素。默认情况下，安全组允许所有出站连接。

客户负责为 PCI DSS 合规配置特定的出站连接规则（configuring specific outbound connection rules）。网络 ACL（Network ACLs） 是 VPC 的可选安全层，是控制一个或多个子网进出流量的无状态 NSC。

您可以进一步使用 IAM 策略（IAM policies）执行以下操作：

- 根据支持的 亚马逊云科技 服务和资源的策略条件评估和拒绝流量
- 包括 VPC 端点
- 在您的环境中执行 NSC 功能

VPC 端点（VPC endpoints）是 VPC 的一项功能，使您能够使用私有 IP 地址连接到受支持的 亚马逊云科技 服务。VPC 端点服务由 亚马逊云科技 PrivateLink 提供支持。该流量不会离开 亚马逊云科技 网络，不需要互联网访问或公共 IP 地址即可与通过 VPC 端点暴露的资源通信。亚马逊云科技 API 默认使用 TLS 加密传输到端点的数据，因此创建此私有网络路径对于合规性不是必需的。

然而，VPC 端点对于设计符合 PCI DSS 的网络很有用，因为它们简化了证明 VPC 资源与 亚马逊云科技 服务之间的数据不会穿越开放的公共网络，符合 PCI DSS 要求条款 4.1。

如果您使用第三方虚拟设备，可以使用弹性负载均衡服务（Elastic Load Balancing）的网关负载均衡器（Gateway Load Balancer）来强制部署 DMZ 区域 并支持限制入站和出站流量，以满足要求条款 1.3.1 和 1.3.2。网关负载均衡器可用于将入站和出站流量路由到您的虚拟设备，支持要求条款 1.4，并为您提供一个网关，用于在多个虚拟设备之间分配流量。

1.4 限制可信和不可信网络

VPC 网络功能包括一个映射服务，该服务执行检查，确保有格式错误或修改过的地址的数据包不能跨越 VPC 边界，满足 VPC 托管环境的要求条款 1.4.3。公共弹性 IP 地址接收的流量被路由到 EC2 网络，并在 EC2 实例接收之前受到这些相同的网络控制。

亚马逊云科技 服务端点（Amazon service endpoints）是具有公共 IP 地址的 Web 服务接口，其安全和合规性由 亚马逊云科技 负责。它们作为 亚马逊云科技 评估的一部分针对 PCI DSS 要求条款进行评估。客户可以确信，这些 亚马逊云科技 服务 API 端点是不可信网络和可信网络之间的合规网络边界，以及可信网络内的分段(例如 DMZ 和内部网络之间)。

您可以使用 亚马逊云科技 端点和 API，如 CloudFront 或 Amazon API Gateway（Amazon API Gateway,），满足要求条款 1.4、1.4.1、1.4.2 和 1.4.4，在客户 VPC 资源(如 RDS)的前端部署 DMZ 区域 或其他网络安全控制，并结合适当的 IAM 限制和其他安全控制，禁止直接公共访问。

要求条款 2

要求条款 2 专注于保护系统组件并确保只有必要和可信的软件在这些系统上运行。亚马逊云科技提供多种服务来支持这一点，并提供服务部署指导以协助以安全方式配置资源。

2.2 Configuration standards

客户负责维护在 亚马逊云科技 上配置的资源的安全配置标准。这些标准必须与行业认可的系统加固标准一致，并包括客户对 亚马逊云科技 服务的配置。亚马逊云科技 已为环境和各个服务发布了广泛的安全指南。这些基本指南包括：

- 亚马逊云科技 良好架构框架：安全支柱 （Amazon Well-Architected Framework: Security Pillar）
- 互联网安全中心（Center for Internet Security (CIS) Benchmark for 亚马逊云科技）
- 安全身份和合规性最佳实践（Best Practices for Security, Identity, & Compliance
- 亚马逊云科技 Trusted Advisor（Amazon Trusted Advisor）
- 改善亚马逊云科技账户的 10 大安全措施 （Top 10 security items to improve in your 亚马逊云科技 account）

亚马逊云科技 安全配置的其他支持可在安全学习页面（the Security Learning）、亚马逊云科技 Skill Builder（Amazon Skill Builder） 和 亚马逊云科技 服务特定文档中获取。

使用亚马逊云科技托管和抽象服务的客户在满足这项要求方面承担的责任大幅减少，在某些情况下，使用这些服务甚至可以完全消除特定系统组件对某些要求的适用性。例如，如果您使用 Lambda 函数，您将不再需要负责满足要求 2.2.3，这是因为该服务本身就是为此目的而设计构建的。

客户完全配置客户管理的实例。客户的责任包括：

- 操作系统、网络和应用程序层面的配置和功能的合规性
- 遵循供应商指导、行业最佳实践和 亚马逊云科技 对系统加固的建议

- 安全配置

客户定义的实例还包括来自 亚马逊云科技 Marketplace 的亚马逊机器映像(Amazon Machine Images (AMIs))。亚马逊云科技 Marketplace 提供由亚马逊合作伙伴网络(Amazon Partner Network (APN))合作伙伴预配置的 AMI，这些 AMI 已由安全专业人员加固以满足 PCI DSS 标准。

亚马逊云科技 还提供其他服务，这些服务不存储、处理、传输或直接影响账户数据的安全性，但可以帮助客户管理其 CDE 中的系统组件。Systems Manager 和 亚马逊云科技 Config 是托管服务，可提供 亚马逊云科技 资源清单、配置历史记录和配置变更通知，以支持安全和治理。亚马逊云科技 Config 规则支持自动检查亚马逊云科技 资源配置（automatic checks of 亚马逊云科技 resources configurations）。

客户可以使用 亚马逊云科技 Config 保持资源处于安全配置状态，并负责管理在服务内配置的权限。客户还可以使用 亚马逊云科技 托管服务(Amazon Managed Services (AMS))以合规方式代表他们操作其 亚马逊云科技 资源（但请注意，合规性仍然是客户的责任）。AMS 提供常规基础设施操作，如补丁管理、连续性管理和安全管理。它还提供 IT 管理流程，如事件、变更和服务请求管理。

2.2.2 更改供应商默认设置

客户负责更改任何集成到其 亚马逊云科技 环境中的第三方软件和代码中的供应商提供的默认设置。亚马逊云科技 服务没有默认账户或凭证。客户必须使用 IAM 和 亚马逊云科技 IAM Identity Center（亚马逊云科技 IAM Identity Center (successor to Amazon Single Sign-On),）、Amazon Cognito（Amazon Cognito）、亚马逊云科技 Directory Service （亚马逊云科技 Directory Service,）或其他授权机制配置他们想要的访问权限。

客户负责配置对 EC2 实例的操作系统级访问（operating-system–level access to EC2 instances）及其配置。客户可以使用 EC2Config（EC2Config） 服务配置其 Windows 实例，该服务为管理员账户（administrator）设置随机加密密码。客户还可以使用 Amazon Linux 实例，默认情况下禁用密码认证（password authentication disabled by default），并在启动时需要密钥对。通过 亚马逊云科技 Organizations（Amazon Organizations,） 创建成员账户

（creating member accounts）时，Organizations 最初为根用户分配至少 64 个字符长的密码，且无法检索。客户必须使用密码恢复功能并设置自己的密码。

亚马逊云科技 在公共文档中为每项服务提供供应商安全指导。指导包括 API Gateway 的安全使用（secure use of API Gateway）以及使用 亚马逊云科技 访问密钥（Amazon access keys）和签名（signed requests.）请求。

2.2.7 非控制台管理

亚马逊云科技 资源的管理被视为此要求条款的非控制台管理，必须使用加密连接，如 SSH、HTTPS 或 VPN。这包括使用 亚马逊云科技 管理控制台（亚马逊云科技 Management Console）管理资源。客户负责确保对其在 亚马逊云科技 中部署的资源的这些管理连接的安全性。例如，如果客户将应用程序部署到 EC2，如入侵检测系统(IDS)或虚拟防火墙，他们还必须确保不安全的服务（如 HTTP 或 FTP）不能用于执行管理功能。

管理员用于访问 亚马逊云科技 管理控制台、亚马逊云科技 CLI（Amazon CLI,） 或服务 API 的系统容易受到凭证窃取、数据泄漏和其他数据风险。它们应被视为可能影响 CDE 安全性的系统。有必要确定哪些系统可以访问 亚马逊云科技 管理控制台（determine which systems can access the 亚马逊云科技 Management Console）并运行 亚马逊云科技 CLI 命令（Amazon CLI commands），以限制评估范围。

客户负责确保在用于通过 亚马逊云科技 管理控制台管理资源的工作站和其他设备上实施技术控制，并根据 NIST 800-52 Rev. 2 （NIST 800-52 Rev. 2）和其他行业最佳实践强制使用强加密。

您可以使用 Systems Manager（Session Manager） 在 EC2 实例上执行管理功能，并充当类似于堡垒主机（也称为跳板机）的角色：一个设计用于管理从不受信任网络到受信任网络的访问的系统。Systems Manager 的 Session Manager 功能允许您让服务代理与 EC2 实例的连接，而无需将 VPC 网络开放给外部流量。在此场景中，要求条款 1.3 可以通过 Systems Manager 服务仅支持到 亚马逊云科技 服务端点（如 ssm.us-east-2.amazon 亚马逊云科技.com）的 HTTPS 连接来解决。

用户和角色必须在允许连接之前由 IAM 明确授权和验证，因此唯一的连接是从终端用户或管理员主机到 亚马逊云科技 服务端点，然后 亚马逊云科技 服务处理与私有 VPC 中各自 EC2 实例的连接。由于 Systems Manager 是完全托管的服务，且流量存在于应用程序层，IAM 权限边界可作为网络安全控制，支持符合要求条款 1.4。

要求条款 3

亚马逊云科技 为大多数存储服务提供静态加密功能，包括 Amazon 关系型、键值、文档、图形和分类账数据库(Amazon relational, key- value, document, graph, and ledger databases)、Amazon ElastiCache for Redis(Amazon ElastiCache for Redis) 和 S3。客户有责启用加密并维护强大的数据保留政策和程序，其中包括在授权完成后不存储或记录敏感账户数据(SAD)。

您可以使用 Amazon Key Management Service (Amazon KMS) 或 Amazon CloudHSM 服务简化要求条款 3.6 和 3.7 所涉及的密钥材料的创建和管理工作，并使用 IAM 强制实施精细的访问限制。您应该使用 KMS 客户托管密钥(CMK)对账户数据进行加密，这些密钥是 256 位高级加密标准(AES)对称密钥，不可导出，并被视为 PCI DSS 附录 G 中定义的强加密。客户还可以使用 Amazon Macie 帮助发现、分类和保护存储在 S3 中的敏感数据。

3.2 账户数据存储保持最小化

客户负责通过数据保留和处置政策确保账户数据存储保持最小化，并实施机制确保不再需要的账户数据被移除。DynamoDB 生存时间(DynamoDB Time to Live (TTL))功能允许客户配置每个项目的 TTL，可用于账户数据，当时间到期时，DynamoDB 会从表中删除该项目，而不消耗写入吞吐量。

3.3 账户数据存储保持最小化

客户负责确保授权后不保留 SAD，并在授权完成前使用强加密对其进行加密。

3.5 静态数据加密

客户可以使用具有 CMK 功能 的 KMS 来减轻其合规负担，通过在存储时使账户数据不可读取，来满足要求条款 3.5.1 和 3.5.1.1。PCI DSS v4.0 通过要求条款 3.5.1.2 引入了增强的静态加密要求。该要求规定，如果使用磁盘或分区级加密来保护 PAN，而不是文件、列或字段级数据库加密，则还必须通过另一种机制进行保护。当客户使用 亚马逊云科技 托管和抽象服务（如 RDS 或 S3）时，底层磁盘和操作系统对您是抽象的，由 亚马逊云科技 管理。客户负责应用层数据的加密，例如使用 RDS 时的数据库加密。客户还可以使用 S3 存储使用 KMS CMK 加密的账户数据，结合 S3 存储桶策略（S3 bucket policies）和 IAM 策略限制访问并根据此要求保护数据。在此场景中，所有加密都是对象(文件)级别的。当客户使用 亚马逊云科技 抽象服务时，不会接触到操作系统认证及相关磁盘。

3.6 和 3.7 密钥管理

客户还可以使用 KMS 来遵守密钥管理要求。KMS 密钥(包括非对称 KMS 密钥的私钥)不能以明文形式从 HSM 导出。它们的整个生命周期都在 KMS 内。只有非对称 KMS 密钥的公共部分可以从控制台导出或通过调用 GetPublicKey API 导出。这意味着 亚马逊云科技 部分负责管理 KMS 内用于保护账户数据的底层加密密钥和 HSM。

客户负责通过密钥和 IAM 策略控制对 KMS 服务功能的访问以满足要求条款 3.5.1 和 3.5.1.3，为要求条款 3.6.1.1 和 3.7.4 定义加密周期（cryptoperiods），并维护管理 KMS 服务用于创建、轮换和删除密钥的策略和流程。当客户使用 KMS 客户托管密钥(CMK)且不导入自己的密钥材料时，亚马逊云科技 具有以下责任：

- 根据要求条款 3.6.1.2 和 3.6.1.4 进行安全密钥存储
- 当客户在 KMS 服务内启动时的特定密钥生成活动
- KMS 服务内的密钥分发
- 当客户启动时根据要求条款 3.7 销毁密钥

亚马逊云科技 还提供 CloudHSM，这是一个 通过了 FIPS 140-2 level3 级验证的基于云的硬件安全模块(HSM)，用于在 亚马逊云科技 云中生成和使用加密密钥。使用 CloudHSM 时，您保留密钥分发和管理的责任。

KMS 和 CloudHSM 都可以生成和维护使用中的加密密钥清单，以符合要求条款 3.6.1.1。

要求条款 4

客户负责配置 亚马逊云科技 作为服务选项提供的强加密和安全控制。暴露到外部的 亚马逊云科技 服务，如 Amazon CloudFront、Amazon API Gateway,和弹性负载均衡器，支持使用 TLS 1.2 或更高版本的传输加密级别，并可以实施策略来强制执行。客户负责选择要求至少 TLS 1.2 的弹性负载均衡器安全策略。安全组和网络 ACL 可以阻止使用不安全的协议。您可以使用 CloudFront 字段级加密（field-level encryption）添加额外的安全层和 HTTPS 来保护整个处理过程中的特定数据。

客户负责确保客户端和服务器协商并使用强 TLS 密码，以符合要求条款 4.2.1.b 和 4.2.1.c。

客户网关、虚拟私有网关、中转网关和 VPN 连接使您能够设置加密的 VPN 隧道进入 VPC，确保流量不会在开放的公共网络传输。

您还可以实施 VPC 端点（VPC endpoints），通过 Amazon PrivateLink 私密连接 VPC 到支持的 亚马逊云科技 服务和 VPC 端点服务，确保流量不离开 亚马逊云科技 网络。通过 PrivateLink 驱动的端点从您的 VPC 离开到 亚马逊云科技 服务的流量不在要求条款 4.2 的范围内。

Amazon Direct Connect 连接是专用的物理网络连接到 亚马逊云科技，默认情况下在客户环境和 亚马逊云科技 之间不加密。客户必须验证网络连接的隐私性，并确定是否需要额外的控制措施来符合要求条款 4.2。

您可以使用 Amazon Certificate Manager (ACM)为 亚马逊云科技 服务和内部连接的资源（如 CloudFront、API 和 API Gateway 以及弹性负载均衡器）配置、管理和部署 SSL/TLS 证书。Certificate Manager 还可用于生成和维护使用中的证书清单以及与要求条款 4.2.1.1 和 12.3.3 相关的信息。

亚马逊云科技 SDK 使用由调用客户端应用程序配置的 HTTPS。由于某些 亚马逊云科技 端点继续支持 TLS v1.0，如果使用公共 亚马逊云科技 端点，客户端应使用其编程语言的 SSL 库配置提供的 TLS 协议(TLS v1.2 及更高版本)。例如，请参阅配置 Python 的 SSL/TLS 参数的说明（instructions for configuring SSL/TLS parameters for Python）。Amazon Java SDK、Amazon SDK for JavaScript、the Amazon SDK for Ruby、Amazon SDK (boto3) 和 Amazon CLI 也提供了其他说明。

要求条款 5

亚马逊云科技 负责为 亚马逊云科技 托管服务（如 Amazon RDS、Amazon ECS 和 亚马逊云科技 Fargate）的底层资源提供病毒防护和反恶意软件保护。您可以继承 亚马逊云科技 PCI DSS 评估为 亚马逊云科技 托管服务提供的安全性和合规性。客户负责在其管理底层操作系统的任何适用 EC2、容器或其他计算实例上配置和运行适当的反恶意软件。亚马逊云科技 Marketplace 为客户提供了众多可使用的产品。

Amazon GuardDuty 恶意软件保护功能（Amazon GuardDuty Malware Protection,）启用后，可以对检测到可疑行为的 EC2 实例和容器工作负载进行自动扫描，并且可以在 GuardDuty 控制台中查看发现结果。这可以帮助客户满足要求条款 5.2.2 中关于恶意软件检测的要求，但客户负责通过实施各种执行机制来移除、阻止或隔离 GuardDuty 检测到的恶意软件。

要求条款 6

6.2 Secure software development

亚马逊云科技 负责 亚马逊云科技 服务和功能的安全开发。客户负责其在 亚马逊云科技 云上开发的应用程序、软件开发实践以及培训员工。

您可以使用 as Amazon CodeStar, Amazon X-Ray, Amazon CodeCommit, Amazon CodePipeline, Amazon CodeBuild, 和 Amazon CodeDeploy 等服务来改进和补充您的实践。每项服务都可以被纳入持续集成和持续部署(CI/CD)流程中。

客户有责任确保在软件开发生命周期的每个阶段进行适当的测试、验证和批准（无论是手动还是自动化的），以满足要求条款 6.2 下的要求。这包括 Lambda 函数的代码、浏览器脚本和基础设施即代码逻辑，如实现应用程序功能或合规控制的 亚马逊云科技 CloudFormation 模板或 亚马逊云科技 Config 规则。

亚马逊云科技 Marketplace 为您提供解决方案，如 SonarQube 或 Snyk，以满足要求条款 6.2.4 中关于识别常见编码漏洞的要求。您可以使用 Amazon CodeGuru 识别代码中更复杂的问题，并提出与数据泄漏预防或安全分析等建议类型相关的改进建议。

6.3.1 安全漏洞

客户负责建立一个识别安全漏洞的流程，并为新发现的安全漏洞分配风险等级。Amazon Inspector 是一项自动化安全评估服务，有助于提高部署在 亚马逊云科技 上的应用程序的安全性和合规性，可以协助您识别潜在风险。Amazon Elastic Container Registry (ECR)提供镜像扫描功能（image scanning），帮助识别容器镜像中的软件漏洞。亚马逊云科技 发布安全公告（security bulletins），通知客户重要的安全事件。您还可以在 亚马逊云科技 Marketplace 中找到来自 Rapid7、Qualys 和 Tenable 等行业认可供应商的众多即用型解决方案。

6.3.3 关键安全补丁

除非在 Amazon Artifact 上的 亚马逊云科技 PCI 责任摘要中另有说明，否则客户负责对其在 EC2 实例和容器上部署的系统和应用程序进行补丁修复。来自 亚马逊云科技 Marketplace 的产品也可能需要打补丁。您可以使用 Systems Manager Patch Manager 自动维护和部署补丁及更新到您的 EC2 实例。AMS 也可用于为您管理补丁活动。

6.4 Web 应用程序保护

您可以使用 亚马逊云科技 WAF 作为自动化技术解决方案来检测和防止基于 Web 的恶意活动。要求条款 6.4 的测试程序规定，"检测和防止基于 Web 攻击的自动化技术解决方案"必须"尽可能保持最新"。您可以通过 亚马逊云科技 Web 应用程序防火墙的托管规则（Managed Rules for Amazon Web Application Firewall）或 亚马逊云科技 Marketplace 托管规则服务来满足此要求。除此之外，客户仍然有责任使用手动或自动化的应用程序漏洞安全评估工具或方法来审查面向公众的 Web 应用程序，这种审查至少应每年进行一次，并且在进行任何变更后也需要进行。

6.5 变更管理

亚马逊云科技 建议客户使用单独的生产和非生产 亚马逊云科技 账户和 VPC，以支持满足要求条款 6.5.1。亚马逊云科技 完善架构框架的安全支柱为客户提供了通过使用 IAM 实施基于角色的访问控制来分离访问的指导。客户还可以使用 AMS 代表他们运营其 亚马逊云科技 环境，以解决要求条款 6.5.1、6.5.3 和 6.5.4 的部分内容。

根据要求条款 6.5，客户最终负责其变更管理操作。

要求条款 7

要求条款 7 的大部分内容都由客户的访问管理策略和实际操作。客户有责任管理其 亚马逊云科技 资源，例如通过其访问管理体系，以满足这些强访问控制要求。

您可以使用 IAM 向您的 亚马逊云科技 账户中的用户和服务授予访问权限。为了符合 PCI DSS，您必须遵循要求条款 7.2.5 中的最小权限原则，我们还建议为要求条款 8.4 启用 亚马逊云科技 管理控制台访问的多因素身份验证。您可以使用服务控制策略（service control policies）确保 亚马逊云科技 账户遵循组织的访问控制准则。

您有多种选择将访问管理和控制扩展到其他本地或其他环境：Cognito、Amazon RDS 身份联合（Amazon RDS identity federation,）、IAM 联合服务（IAM federation services,）、IAM Identity Center 和 Amazon Directory Service。

7.2.4 访问审查

您可以为账户中的用户生成凭证报告，并查看其各种凭证的状态，以审查谁被授予了环境访问权限。您还可以使用 IAM Access Analyzer 识别对资源和数据的非授权访问，这可能构成安全风险。

7.2.数据库访问

应使用安全组、网络 ACL 和 IAM 角色来限制对数据库的访问，只允许必要的应用程序和服务器查询 RDS 数据库，以帮助防止外部或未授权访问的可能性。您可以使用 Amazon Secrets Manager 安全地存储数据库凭证，并确保数据库应用程序的应用程序账户不能被个人用户或其他非应用程序流程使用。

客户负责在其部署的数据库实例中建立自己的数据库引擎身份和角色。IAM 数据库身份认证（IAM database authentication）允许用户和账户连接到 RDS 数据库，可以简化满足此要求的过程。

7.3.3 默认拒绝

亚马逊云科技 服务中定义的权限，无论是在 IAM 还是 S3 存储桶或 KMS 密钥策略中，都在策略评估逻辑（policy evaluation logic.）中包含默认的"拒绝所有"。

要求条款 8

要求条款 8 深入探讨了访问管理的细节，即如何在 CDE 内配置和管理访问权限和用户。亚马逊云科技提供了 Access Analyzer、IAM Identity Center、Organizations 和 Secrets Manager 等服务，帮助解决 CDE 中要求条款 8 的部分内容。多因素认证(MFA)也得到支持，以强制安全访问您的 CDE，满足要求条款 8.4 和 8.5。与要求条款 7 类似，您有多种选择将访问管理和控制扩展到本地或其他环境。

8.2.2 分段隔离, 共享或通用账户

客户应仅在必要时基于例外情况并有书面业务理由和批准的情况下允许共享凭证。客户可以使用 Secrets Manager 安全存储必须共享的凭证，该服务将活动记录在 CloudTrail 审计跟踪中。

客户必须采用最小权限原则授予用户访问权限，包括实施密码要求和 MFA。对亚马逊云科技服务的编程访问（包括 API 调用）应使用 IAM 角色执行，使用亚马逊云科技 Security Token Service 颁发的临时和有限制权限凭证。

8.2.6 删除 90 天内不活跃的用户账户

客户负责识别不活跃的用户账户，并在 90 天无活动后删除或禁用它们。客户可以为其账户中的用户生成凭证报告（credential reports），以及其各种凭证的状态，以审查账户并识别最近未使用的账户。客户还可以设置自动化并使用 Lambda 和 CloudWatch 等服务来完成这些任务和需求。

应建立程序或自动化机制，以识别并在 90 天内删除或禁用不活跃的 IAM 账户。客户可以选择使用亚马逊云科技服务实现这一点，使用外部客户管理源的身份联合，或使用亚马逊云科技 Directory Service。

8.2.7 第三方访问

客户可以使用 IAM 策略权限集（permission sets）来设置会话持续时间并控制用户可以登录亚马逊云科技账户的时长，以限制第三方的访问。

8.2.8 空闲回话超时

客户负责实施和强制空闲会话超时，可以使用 Systems Manager Session Manager 对 Systems Manager 服务代理的会话强制执行要求。客户还需要通过外部身份提供商或亚马逊云科技 Managed Microsoft Active Directory 组策略在用户工作站上强制执行 15 分钟的空闲会话超时要求。这通常通过终端用户工作站上的用户屏幕保护程序锁定计时器来实现。特权控制台访问的最佳实践是将流量限制到特定工作站以限制范围，并配置这些工作站以强制执行空闲会话超时。

8.3 用户认证和管理

客户有责任确保其 IAM 密码策略配置（IAM password policy）为强制使用至少 12 个字符长度的密码，包含字母和数字或非字母数字字符、90 天或更短的过期时间，并防止重复使用最近四个或更多密码。客户可以选择使用亚马逊云科技服务实现这一点，使用外部客户管理源的身份联合，或使用亚马逊云科技 Directory Service。这些解决方案可用于帮助满足许多账户和密码要求。

亚马逊云科技身份存储（包括但不限于 IAM、Cognito 和亚马逊云科技 Directory Service）安全地存储和传输所有凭证，并在使用这些服务时代表客户满足要求条款 8.3.2。亚马逊云科技建议使用 IAM 角色进一步限制对离散用户账户的需求，并使用 Amazon Simple Notification Service (SNS)主题通知异常行为。

8.3.4 账户锁定

亚马逊云科技管理控制台没有机制来强制执行 PCI DSS 所需的设置。IAM 本身不支持账户锁定。对于确定在 PCI DSS 评估范围内的 IAM 用户，需要额外的机制来满足要求条款 8.3.4 账户锁定要求。客户

可以通过联合身份提供对亚马逊云科技资源的访问，并使用其现有的第三方身份提供商或亚马逊云科技 Managed Microsoft AD 执行账户锁定功能。

8.5.1 多因子认证

亚马逊云科技身份服务（如 IAM、Cognito 和 IAM Identity Center）提供的多因素认证功能的安全性是亚马逊云科技作为共享责任模型中云安全组件的责任，满足要求条款 8.5.1。

IAM 策略对亚马逊云科技管理控制台、亚马逊云科技 CLI 和 API 访问强制执行 MFA 要求，以满足要求条款 8.4。亚马逊云科技最佳实践是所有新的 IAM 用户都配置为访问亚马逊云科技管理控制台、亚马逊云科技 CLI 或相关 API 时需要 MFA。

8.6.2: 密码不硬编码到可部署代码中

客户可以使用 Systems Manager Parameter Store 或 Secrets Manager 存储密码和敏感信息，然后由应用程序在必要时检索。存储在 Parameter Store 和 Secrets Manager 中的敏感数据可以使用客户 KMS 密钥进行加密。

要求条款 9

亚马逊云科技管理托管环境的物理基础设施，物理安全要求继承自亚马逊云科技全球基础设施。对于 PCI DSS 要求条款 9.4，客户负责从亚马逊云科技环境导出或传输出的媒体的物理安全和数据分类，但不负责存储在亚马逊云科技内的数据的物理安全。根据 PCI DSS 要求条款 9.5，客户负责用于连接到亚马逊云科技云中配置资源的物理支付设备的物理安全和管理。客户还负责存储、处理或传输账户数据的任何物理位置的安全，这些位置可能包括公司办公室、呼叫中心或零售店。

使用 Outposts 和 SnowFamily 设备的客户负责确保为第 9 项要求条款实施适当的物理控制措施，因为这些控制措施不能从亚马逊云科技全球基础设施继承。

要求条款 10

亚马逊云科技提供许多特定于服务的安全和审计日志，以帮助客户满足其合规需求。考虑到这一点，应该有控制措施确保账户数据不会出现在日志和调试文件中。

10.2 实施审计日志记录

Amazon CloudTrail 提供支持的亚马逊云科技区域（supported Amazon Web Services Regions）中亚马逊云科技服务（Amazon Web services）的亚马逊云科技账户 API 活动的事件历史记录，包括通过亚马逊云科技管理控制台、亚马逊云科技 SDK 和命令行工具执行的操作。这些日志包含满足要求条款 10.2.2 所需的六个详细信息，用于跟踪与审计在亚马逊云科技环境活动，并可将日志传送到 S3 进行安全存储和分析。

客户可以使用 CloudWatch 记录由 Lambda 函数处理的请求。客户还负责在代码中插入适用的日志记录语句，以记录应用程序内的账户数据访问和管理活动。客户还可以在 EC2 实例上安装 CloudWatch 代理，以收集额外的系统级指标，这些指标可用于将操作系统的日志发送到 CloudWatch Logs 服务进行保留。如果用于部署 EC2 实例的 AMI 没有预安装 CloudWatch 代理，客户可以自行安装（install）以提供额外的日志记录功能。制定日志记录策略（logging strategy）将有助于确保适当的请求被记录到 CloudWatch 中。

客户负责为其部署的每个范围内的 RDS 实例识别和配置所需的审计日志设置。这包括在 Amazon Aurora（Amazon Aurora） MySQL 中启用高级审计功能（Advanced Auditing）或在 Amazon RDS MySQL 中使用 MariaDB 审计插件。客户还负责从其容器化基础设施中收集审计日志。这可能包括在 Amazon Elastic Kubernetes Service (Amazon EKS)中启用控制平面日志（control plane logs）。

在 S3 中存储账户数据的客户应启用和配置 CloudTrail 数据事件，以获取 S3 中存储桶和对象级请求的信息。如果启用了 S3 静态网站托管，还应启用和配置 S3 服务器访问日志记录，以捕获 S3 对象级活动和身份验证失败（authentication failures）。

10.3 保护审计日志

客户应使用精细的 IAM 策略限制 S3 和 CloudTrail 访问，并且只允许特定信息安全人员访问审计跟踪。另外这两项服务还支持使用版本控制、生命周期策略和拒绝删除功能来保护日志数据。客户可以使用 S3 对象锁定来保护存储在 S3 存储桶中的审计跟踪，该功能使用一次写入多次读取(WORM)模型存储对象。

对象锁定可以帮助防止对象在固定时间内或无限期地被删除或覆盖。当客户启用 CloudTrail 后，还提供日志文件完整性验证功能（log file integrity validation feature），满足这些审计跟踪的要求条款 10.3.4。

10.4 审查审计日志

客户有许多选项和工具可用于审查安全事件和审计跟踪，并负责实现要求条款 10.4.1.1 所需的自动审查机制。亚马逊云科技规范性指导门户提供了策略（Amazon Prescriptive Guidance）、指南和模式，可以帮助客户确定满足其需求的解决方案。一个例子是使用 Amazon Athena 和 Amazon QuickSight.可视化 Amazon Redshift 审计日志（visualize Amazon Redshift audit logs）。亚马逊云科技 Marketplace 还提供了几种 SIEM 选项（offers several SIEM options.）。

对于要求条款 10.4.2，查看所有其他系统组件的日志，客户可以使用 Athena 查询保存在 S3 中的审计跟踪日志。您可以使用 Lambda 将日志数据从 CloudWatch 加载到 Amazon OpenSearch Service，并使用 Kibana 或 OpenSearch Dashboards 界面和 REST API 进行可视化。GuardDuty 和 Amazon Security Hub 可以结合使用，提供自动事件分析，并可以通过 CloudWatch Events 和 Lambda 实现自动修复。客户还可以配置 CloudWatch 警报（send alerts through Amazon SNS），在 CloudTrail 日志中识别到根账户使用时通过 Amazon SNS 主题发送警报。

10.5 保留审计日志

客户应使用专用 S3 存储桶保留审计日志跟踪，并可以配置生命周期策略（lifecycle policies）将超过三个月的数据迁移到 S3 Glacier 以节省成本。将 Amazon CloudWatch 日志导出到 S3（Exporting Amazon CloudWatch logs to S3）还可以通过加密（encryption）保护日志数据并防止或检测更改（prevent or detect changes）。如果 S3 作为组织的官方审计跟踪来源，可以使用 S3 对象锁定来支持 12 个月的保留要求，限制意外或恶意删除日志文件的操作。

10.6 时间同步(NTP)

亚马逊云科技提供 Amazon 时间同步服务（Amazon Time Sync Service），可以为 EC2 实例（set for EC2 instances）和容器设置，也被其他亚马逊云科技服务使用。该服务使用每个区域中连接卫星和原子参考时钟的集群，通过网络时间协议(NTP)提供协调世界时(UTC)全球标准的准确当前时间读数。

时间同步服务会自动平滑添加到 UTC 的任何闰秒。可以通过链接本地的 169.254.169.123 IP 地址访问此服务。这意味着不需要配置外部互联网访问，并且可以从私有子网内安全地访问该服务。

10.7 Critical security control failures

客户负责确保为其关键安全控制和系统实施某种形式的监控和警报，并确保及时检测和解决故障。除了前面描述的警报监控选项外，客户还可以使用亚马逊云科技 Config 创建自定义规则（Amazon Config custom rule），评估其记录资源的合规信息。可以创建亚马逊云科技 Config 自定义规则来监控（monitor for Amazon resource changes）被识别为关键安全控制的资源，当检测到更改时，亚马逊云科技 Config 可以向 SNS 主题（send notifications to an SNS topic）发送通知。

同时客户还可以使用 Amazon 简单队列服务(Amazon Simple Queue Service)或 Amazon EventBridge 监控亚马逊云科技资源变更。

最后客户还可以将其安全警报汇总到 Security Hub 中，并使用 Security Hub 检查来监控亚马逊云科技 Config 资源的变更。

要求条款 11

客户负责第 11 项要求条款的大多数方面，并可以使用多种亚马逊云科技服务来帮助解决系统和网络安全测试的不同方面。Amazon Inspector 是一项出色的漏洞扫描服务，可支持要求条款 11.3.1 和内部漏洞扫描；GuardDuty 是一个优秀的入侵检测系统，可支持符合要求 11.5；亚马逊云科技 Config 可以帮助客户检测未授权访问，以符合要求条款 11.5.2。客户负责确保所有安全工具都正确配置，能够在安全事件发生时提醒人员，并确保按照要求条款解决漏洞问题。

11.2.1 无线接入点

亚马逊云科技管理亚马逊云科技云的物理基础设施，亚马逊云科技管理设施的无线网络控制继承自亚马逊云科技全球基础设施。客户负责对其非云基础设施进行恶意无线接入点扫描，但不需要对其基于亚马逊云科技的 CDE 进行此类扫描。

11.3 内部和外部扫描

亚马逊云科技可接受使用政策（Amazon Web Services Acceptable Use Policy）描述了亚马逊云科技上允许和禁止的行为，包括对禁止的安全违规和网络滥用的描述。亚马逊云科技客户可以在不需要事先批准的情况下，针对八种服务对其亚马逊云科技基础设施进行安全评估或渗透测试。所有渗透测试人员和漏洞扫描管理员应了解并遵守亚马逊云科技渗透测试的客户支持政策（Amazon Web Services Customer Support Policy for Penetration Testing.）。

客户可以使用 Inspector 快速发现 EC2 实例、容器和 Lambda 函数等计算工作负载中的漏洞。根据要求条款 11.3.1.2，Inspector 扫描被视为已认证扫描。扫描是从客户的操作系统内部进行的。如果客户有多账户结构，Inspector 的发现可以发送到 Security Hub 以获得集中视图。客户可以参考 CVE 网站（CVE site），查看 Amazon Inspector 扫描（Amazon Inspector scan.）中发现的常见漏洞和暴露。CVE 网站允许客户获取有关 CVE 的详细信息、其严重性以及如何缓解它。

> 注意：客户不允许对亚马逊云科技基础设施或亚马逊云科技服务本身进行任何安全评估。如果您怀疑任何亚马逊云科技服务存在安全问题，请立即联系亚马逊云科技安全团队。

客户负责聘请获批准的扫描供应商(ASV)进行外部漏洞扫描，以符合要求条款 11.3.2。目前亚马逊云科技不提供 ASV 服务。

11.4 内部和外部渗透测试

客户可以使用 Amazon VPC Network Access Analyzer（Network Access Analyzer）来支持要求条款 11.4.5 的年度或半年度分段测试。Network Access Analyzer 可以验证处理信用卡信息的系统是否使用了单独的逻辑网络，并且该网络与客户其余范围外环境隔离。

11.5.1 网络入侵测试

软件定义网络（如 EC2 VPC）没有本地 IDS 可以依赖的 OSI 第 2 层物理连接。要求 11.5 规定使用"入侵检测和/或入侵防御技术(IDS 和/或 IPS)来检测和/或防止网络入侵"，并进一步要求监控"CDE 边界以及 CDE 关键点的所有流量，并在怀疑遭到入侵时提醒人员"。

GuardDuty 是一种威胁检测服务，可持续监控恶意活动和未授权行为，以保护您的亚马逊云科技账户和工作负载。客户可以在包含 CDE 资源的亚马逊云科技账户中启用 GuardDuty，以满足要求 11.5.1。客户负责为要求 11.5.1 配置 GuardDuty 事件的警报，例如 CloudWatch Events（CloudWatch Events）。Foregenix 的这份白皮书（whitepaper from Foregenix）记录了他们对 GuardDuty 满足 PCI DSS 入侵检测要求有效性的评估。

客户可以将 GuardDuty 与其他服务结合使用，以增加流量检查功能，例如亚马逊云科技 WAF 或主机入侵检测系统(HIDS)解决方案。

客户还可以通过在其 VPC 中部署 IDS 或 IPS 设备来满足此要求。客户可以配置 VPC 流量镜像（Traffic Mirroring），将流量副本路由到在一个或多个 EC2 实例上运行的虚拟设备。或者，客户可以选择基于主机的 IDS 或 IPS 解决方案，在流量传递到 EC2 实例时对其进行监控。这有一个限制，即客户端无法安装在亚马逊云科技托管实例或 VPC 端点上。亚马逊云科技 Marketplace（Amazon Web Services Marketplace）也提供了各种 IDS 产品。这些产品通常包括其他功能，如文件完整性管理或数据丢失防护，以减少在 EC2 实例上安装多个客户端的需求。

第三种选择是使用传输网络架构，该架构使用 IP 路由确保网络流量穿过单一网络。该选项允许使用亚马逊云科技 Marketplace 中的虚拟防火墙或 IDS/IPS 设备来检查网络间传输的流量。也可以使用 VPC 网关将流量路由到本地 IDS/IPS 基础设施。

11.5.2 变更检测

客户负责为其部署的范围内亚马逊云科技资源以及其维护的操作系统中关键系统文件的变更实施检测和警报。客户可以使用亚马逊云科技 CloudFormation（Amazon CloudFormation）变更检测来检测与客户定义模板不同的 CloudFormation 堆栈变更。亚马逊云科技 Config 是一项服务，使客户能够评估、审计和评估其亚马逊云科技资源的配置。亚马逊云科技 Config 持续监控和记录亚马逊云科技资源配置，并允许客户自动评估记录的配置与所需配置的对比。客户还可以基于 CloudTrail 事件配置警报，以监控客户配置的服务（如 S3）的变更。

对于在处理 PCI 工作负载的 VPC 中部署的容器相关架构，变更检测机制是必要的。亚马逊云科技 Marketplace 还提供了众多第三方解决方案，用于解决传统 EC2 和基于容器的部署中的变更检测和文件完整性监控。

如果客户以只读模式运行容器，使用亚马逊云科技 Fargate 的容器部署不需要客户管理的变更检测。客户只需要 PCI 工作负载的 Lambda 代码部署变更检测机制，可能使用 CloudWatch Logs 和定义的警报，以检测其亚马逊云科技账户内定义身份的未授权变更。亚马逊云科技监控 Lambda 代码，防止来自客户亚马逊云科技账户外部的未授权变更（Amazon monitors Lambda code for unauthorized changes）。Lambda 将代码存储在 S3 中并在静态时对其进行加密。当您的代码在使用中时，Lambda 会执行额外的完整性检查。

11.6 支付页面的变更检测

客户负责为其支付页面实施变更和篡改检测机制。客户可以使用托管在 S3 中的静态网站和只读存储桶，帮助防止页面内容被篡改。

要求条款 12

客户有责任维护其信息安全政策和计划，这些政策和计划为组织安全定调并保护其持卡人数据环境 (CDE)。亚马逊云科技服务如 Amazon Control Tower, Amazon Detective,和亚马逊云科技 Config 提供功能可以减轻管理负担。以下是这些能力的详细说明。

12.2 可以使用的关键技术

亚马逊云科技为客户提供主动限制其账户中使用的应用软件能力。客户可以使用亚马逊云科技 Control Tower 配合服务控制策略来管理部署在其 CDE 中的软件（manage software deployed）。Config 托管规则还为客户提供检查亚马逊云科技 Config 托管实例上应用（blocked applications）的能力。

12.3.1 有针对性的风险分析

客户负责对允许灵活执行频率的 10 项要求条款中的每一项执行针对性风险分析，并覆盖其 PCI DSS 评估范围内的所有适用系统组件。

12.3.2 使用定制方法的针对性风险分析

客户负责确定是否或何时使用定制方法来满足要求，并执行相关的必要针对性风险分析。

12.3.3 加密密码套件和协议

客户可以使用 Certificate Manager 和 KMS 提供正在使用的证书和密钥清单，以展示正在使用的加密密码套件和协议的清单。客户负责在这些清单中添加必要的上下文，包括目的和证书与密钥的使用位置。如果事先知道目的和使用信息，可以将其作为标签添加到加密资源中。这将允许您通过 KMS 服

务的 list-resource-tags API 查询或 Certificate Manager 服务的 list-tags-for-certificate API 查询检索此信息作为证据。

12.5 系统组件清单

客户可以使用 Systems Manager、Amazon Config 和 Application Discovery 服务来支持维护 PCI DSS 范围内的系统组件清单。通过亚马逊云科技 Systems Manager 可以为账户的托管实例收集清单。例如可以通过指定标签或手动方式收集清单。

Systems Manager Agent 默认安装在受支持的亚马逊云科技实例上。您可以使用 Systems Manager Inventory 收集 EC2 实例的操作系统(OS)、应用程序和实例元数据。

亚马逊云科技 Config 可以提供已发现资源的清单，可通过 CLI 或 API 查询。客户还可以使用 CLI、API 或亚马逊云科技管理控制台从相应的集中位置查询每个服务，以生成和报告每个服务实例的清单。

12.8 第三方服务提供商

客户在开设账户并同意使用亚马逊云科技服务时接受的协议包含支持要求条款 12.8.2。亚马逊云科技 Artifact 允许客户按需获取亚马逊云科技 PCI DSS AOC 和责任摘要，以满足亚马逊云科技作为第三方服务提供商的要求条款 12.8.5。

12.9 第三方服务支持

客户可以参考亚马逊云科技客户协议（Amazon Web Services Customer Agreement）第 1.3 节"亚马逊云科技安全"、亚马逊云科技服务条款（Amazon Web Services Service Terms,）第 1.14 节"数据保护"以及隐私声明（Privacy Notice）中的"我们如何保护信息"部分，以支持服务提供商对安全责任的确认。

12.10 事件响应

准备工作对成功的事件响应计划至关重要。亚马逊云科技安全事件响应指南白皮书（Amazon Security Incident Response Guide）为客户提供了在亚马逊云科技云环境中响应安全事件的基础知识概述。亚马逊云科技提供许多安全工具和服务（security tools and services）使组织能够跟踪、

监控、分析和审计事件。客户可以整合亚马逊云科技 Elastic Disaster Recovery（Amazon Elastic Disaster Recovery Service）服务，以支持事件响应计划的业务恢复和保证业务连续性。客户可以在其监控过程中使用 Security Hub，在响应过程中使用 Detective，以支持要求条款 12.10.5。客户应使用 Macie 来检测存储在 CDE 相邻 S3 存储桶中的 PAN，以支持要求条款 12.10.7。

结论

通过过了解亚马逊云科技云环境并适当使用亚马逊云科技服务，可以在亚马逊云科技云中实现合规性。组织可以通过详细的规划及在系统和应用程序的整个生命周期中保持合规意识，从而减轻证明 PCI DSS 合规性的压力。

贡献者

本文档（英文版本）贡献者包括:

- Ted Tanner, Principal Assurance Consultant, Amazon Web Services Security Assurance Services
- Rughved Gadgil, Senior Solutions Architect, Amazon Web Services Worldwide Commercial Services
- Sana Rahman, Senior Assurance Consultant, Amazon Web Services Security Assurance Services

本文档（中文版本）贡献者包括:

- Liu Chunhua, Industry Solution Architect, Amazon Web Services China
- Tan Jing, Industry Specialist, Amazon Web Services China
- Wang QiuYan, Industry Specialist, Amazon Web Services China
- Jason Jiang, Security GTM, Amazon Web Services China
- Fan XunYi, Security GTM Specialist, Amazon Web Services China

附加资源

其他附加资源, 请参考:

- Amazon Web Services Security Assurance Services
- PCI DSS v4.0 Requirements
- PCI DSS v3.2.1 to v4.0 Summary of Changes
- Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms
- PCI DSS v3.2.1 on Amazon Web Services Compliance Guide

- Amazon Web Services Compliance - PCI DSS Level 1 FAQs
- Amazon Web Services Security Documentation
- Amazon Web Services Cloud Audit Academy
- Prowler Open Source security tool

附录

下表描述了本文档中提到的一些亚马逊云科技服务，这些服务在适当配置时可以帮助客户满足各种 PCI DSS 要求。表中包含这些服务的概述以及它们支持的 PCI DSS 要求。亚马逊云科技不断发布新功能并更新服务，以支持亚马逊云科技云中的客户。客户有责任对以下信息进行独立评估。本表：(a)仅供参考，(b)代表当前的亚马逊云科技产品服务和实践，可能会在不通知的情况下发生变更，以及(c)不构成亚马逊云科技及其附属公司、供应商或许可方的任何承诺或保证。亚马逊云科技产品或服务按"原样"提供，不带有任何明示或暗示的保证、陈述或条件。

亚马逊云科技 服务	**支持 PCI-DSS 要求条款**
Security groups 控制允许到达和离开其关联资源的网络流量。	支持要求条款 1.3、1.4 的网络安全控制
Amazon Network Firewall 为您在 Amazon Virtual Private Cloud (Amazon VPC)中创建的虚拟私有云(VPC)提供有状态、托管的网络防火墙和入侵检测与防御服务。	支持要求条款 1.3、1.4 的网络安全控制
Amazon Firewall Manager 安全管理服务，允许您在亚马逊云科技 Organizations 中集中配置和管理跨账户和应用程序的防火墙规则。.	支持要求条款 1.2.7.b、1.2.8 的网络安全控制审查和配置
Amazon API Gateway 完全托管的服务，使开发人员能够轻松创建、发布、维护、监控和保护 API.	支持要求条款 1.4、1.4.1、1.4.2、1.4.4，用于在可信和不可信网络之间实施网络安全控
Amazon Key Management Service (KMS) 让您能够在应用程序和 100 多个亚马逊云科技服务中创建、管理和控制加密密钥。.	支持要求条款 3.5、3.6、3.7 的静态数据强加密和加密密钥管理
Amazon Virtual Private Cloud (Amazon VPC) 使您能够在自定义的虚拟网络中启动亚马逊云科技资源.	支持要求条款 1.3、1.4，限制对持卡人数据环境（CDE）的访问
Amazon Macie 数据安全服务，使用机器学习(ML)和模式匹配来发现并帮助保护敏感数据.	支持要求条款 3.2，确定持卡人数据是否存储在持卡人数据环境之外

Amazon CloudHSM 让您能够在通过 FIPS 验证的硬件上管理和访问密钥，这些硬件由客户拥有的、单租户 HSM 实例保护，在您自己的虚拟私有云(VPC)中运行	支持要求条款 3.5、3.6、3.7 的静态数据强加密和加密密钥管理
Amazon Config 配置工具，帮助您评估、审计和评估资源的配置和关系。.	支持要求条款 2.2、10.7、11.5.2 的安全配置管理和变更检测，以及 12.5.1 的资产清单
Amazon Systems Manager 管理服务，帮助您自动收集软件清单、应用操作系统补丁、创建系统映像，以及配置 Windows 和 Linux 操作系统。.	支持要求条款 2.2 的系统管理，6.3 的补丁管理，8.2.2 和 8.2.8 的安全访问管理，10.2 和 10.3 的会话日志记录，12.5.1 的资产清单
Amazon Certificate Manager 可用于配置、管理和部署公共和私有 SSL/TLS 证书，以便与亚马逊云科技服务和内部连接的资源一起使用。.	支持要求条款 4.2、12.3.3 的强加密和加密清单
Amazon GuardDuty 识别已被恶意软件入侵或存在风险的资源。恶意软件保护支持 GuardDuty 检测可能是入侵源的恶意软件。	支持要求条款 11.5.1 的入侵检测

Amazon CodeStar, 亚马逊云科技 CodeCommit, 亚马逊云科技 CodePipeline 亚马逊云科技 CodePipeline：完全托管的持续交付服务，帮助您自动化发布流程，实现快速可靠的应用程序和基础设施更新。 亚马逊云科技 CodeCommit：安全、高度可扩展、完全托管的源代码控制服务，托管私有 Git 存储库。 亚马逊云科技 CodeStar：提供统一的软件开发活动用户界面，帮助设置完整的持续交付工具链。	支持要求条款 6.2 的安全软件开发
Amazon Inspector 自动化漏洞管理服务，持续扫描亚马逊云科技工作负载中的软件漏洞和意外的网络暴露。	支持要求条款 6.3.1、11.3.1 的漏洞扫描
Amazon WAF Web 应用程序防火墙，让您监控转发到受保护的 Web 应用程序资源的 HTTP(S)请求。.	支持要求条款 6.4 的 Web 应用程序保
Amazon Identity and Access Management (IAM) 允许您指定谁或什么可以访问亚马逊云科技中的服务和资源，集中管理精细权限，并分析访问以优化亚马逊云科技中的权限。	支持要求条款 7、8 的用户和访问管理
Parameter Store 帮助您创建安全、分层的存储，用于配置数据管理和密钥管理。	支持要求条款 3.4.1、8.3.2 的敏感数据安全存储

Amazon Secrets Manager 帮助您在整个生命周期中管理、检索和轮换数据库凭证、API 密钥和其他同加密相关的信息。	支持要求条款 3.4.1、8.3.2 的敏感数据安全存储
Amazon CloudTrail 支持亚马逊云科技账户的治理、合规、操作审计和风险审计。使用 CloudTrail，您可以记录、持续监控和保留与亚马逊云科技基础设施中操作相关的账户活动。	支持要求条款 10.2、10.3 的审计日志记录

文档版本

日期	描述
2023 年 8 月	英文版发布
2025 年 5 月	中文版发布